Circuit pourvu d'un accès externe sécurisé

La présente invention concerne un circuit pourvu d'un accès externe sécurisé.

Le domaine de l'invention est celui des circuits intégrés programmables, notamment celui des circuits utilisés pour réaliser des transactions confidentielles.

Un tel circuit intègre un microprocesseur et, souvent, une mémoire cache, un contrôleur de mémoire cache et / ou une unité de gestion mémoire. Il intègre de plus généralement une mémoire non volatile, une ou plusieurs mémoires de travail telles que mémoire à accès aléatoire (« RAM » pour le terme anglais « Random Access Memory ») ou mémoire à lecture seule (« ROM » pour le terme anglais « Read Only Memory »). Il intègre encore, la plupart du temps, d'autres périphériques propres aux applications qu'il est chargé de mettre en oeuvre.

D'autre part, ce circuit comporte une interface de communication prévue pour un accès externe. Autrement dit, cette interface permet au microprocesseur d'échanger des données avec un quelconque composant localisé en dehors du circuit.

L'invention trouve une application particulièrement avantageuse lorsque ce composant est une mémoire. En effet, il est courant d'adjoindre une mémoire externe au circuit intégré de sorte que les utilisateurs de ce circuit puissent disposer d'un espace mémoire supplémentaire.

Naturellement, le contenu de la mémoire externe est accessible par le microprocesseur, mais il est aussi accessible par n'importe quel autre équipement. Ainsi, il est aisé d'aller lire et même modifier des données enregistrées dans cette mémoire. Or il est parfois impératif que ce contenu ne puisse faire l'objet d'une intervention extérieure au circuit. C'est le cas notamment lorsque la mémoire externe comporte des informations sécuritaires tel qu'un code d'accès confidentiel ou une vérification de signature numérique.

Il est d'ailleurs prévu, lors du chargement d'un programme dans la mémoire externe, que le circuit intégré qui reçoit ce programme de l'extérieur vérifie son authenticité (l'identité de l'émetteur) et son intégrité (l'absence de modification par un tiers) avant de l'enregistrer dans la mémoire. Cette vérification est classiquement réalisée au moyen d'un protocole de signature électronique.

Il est pratiquement impossible d'appliquer ce protocole à chaque fois que la mémoire externe est lue par le circuit intégré car il s'agit là d'une opération qui nécessite une grosse puissance de calcul et qui est par conséquent très lente.

La présente invention a ainsi pour objet de renforcer la protection de cette mémoire externe contre les accès indésirables.

Selon l'invention un circuit comprend un microprocesseur et un ensemble de périphériques comportant au moins une interface de communication prévue pour un accès externe, ces périphériques hormis l'interface de communication étant reliés au microprocesseur par un bus d'interconnexion ; de plus, le circuit comprend un module de sécurisation relié d'une part au bus d'interconnexion et d'autre part à l'interface de communication par l'intermédiaire d'une liaison dédiée.

Suivant un mode de réalisation privilégié du circuit, l'interface de communication est adaptée à une mémoire externe.

Avantageusement, le module de sécurisation comporte des moyens de cryptage CR.

De préférence, ces moyens de cryptage font appel à une clé privée.

Il est souhaitable que la longueur de la clé de cryptage soit supérieure à la longueur standard des données que traite le microprocesseur, si bien que celui-ci comprend des moyens pour décomposer les mots cryptés en données de longueur standard.

Si le circuit comporte de plus une mémoire cache associé à un contrôleur, le module de sécurisation est prévu pour exploiter les accès consécutifs de ce contrôleur afin de décomposer les mots cryptés en données de longueur standard.

Il est préférable que la clé de cryptage soit stockée dans un registre programmable une seule fois, ce registre pouvant figurer dans une mémoire non volatile.

La présente invention apparaîtra maintenant avec plus de détails dans le cadre de la description qui suit d'un exemple de réalisation donné à titre illustratif en se référant à la figure annexée qui représente un schéma d'un circuit intégré selon l'invention.

En référence à la figure, un circuit intégré IC comporte un microprocesseur MIC éventuellement associé à une mémoire cache et/ou à un contrôleur de mémoire (non représentés). Il comporte aussi une interface de

communication UMI et, généralement, d'autres périphériques PER tels qu'une mémoire non volatile de type flash, une mémoire de travail à accès aléatoire etc.

Selon l'invention, le circuit comporte de plus un module de sécurisation CR. Un bus système BUS interconnecte tous les éléments du circuit hormis l'interface de communication UMI, et une liaison dédiée DL relie cette interface UMI au module de sécurisation CR.

En dehors du circuit figure un composant MEM qui peut communiquer avec l'interface de communication UMI et l'invention propose donc de protéger les données qui transitent par cette interface au moyen du module de sécurisation CR.

Dans le cas présent, ce composant est une mémoire externe MEM et l'interface de communication est de préférence une interface mémoire universelle UMI.

Le module de sécurisation CR peut mettre en œuvre différentes techniques pour coder ou modifier les données qu'il reçoit du microprocesseur MIC par le bus système BUS avant de transmettre les données ainsi codées à l'interface de communication UMI, de sorte que celles-ci n'apparaissent pas en clair dans la mémoire externe MEM. Bien sûr, ce module peut procéder au codage inverse lorsqu'il lit des données dans cette mémoire externe MEM afin de les restituer au microprocesseur MIC telles que celui-ci les lui a fournies.

Une solution avantageuse consiste à recourir à des moyens de cryptage qui sont mis en œuvre de préférence par le module de sécurisation CR.

Ainsi, les données sont cryptées avant d'être enregistrées dans la mémoire externe MEM et elles sont décryptées lorsqu'elles y sont lues avant d'être transmises sur le bus système BUS.

Il convient donc de chiffrer les données a la volée avant de les stocker dans la mémoire externe MEM.

Le microprocesseur MIC sait traiter des données de 8, 16 ou 32 bits. Couramment, l'accès à des données externes se fait avec des mots d'une longueur standard de 8, 16 ou 32 bits. Sécuriser de telles données imposerait un cryptage sur 8, 16 ou 32 bits respectivement. Il s'agirait là d'un cryptage très vulnérable, pratiquement inefficace, si l'on emploie des algorithmes connus.

Il est donc souhaitable de choisir un algorithme travaillant sur des données de 64 bits, voire même 128 bits dès lors que cela s'avère nécessaire. La sélection d'un algorithme standard permet d'éviter des contraintes supplémentaires, tout en assurant un niveau de sécurité maximal.

On préfèrera un algorithme a clé privée car il nécessite des temps de calcul beaucoup plus courts qu'un algorithme à clé publique.

A titre d'exemple, on retiendra les algorithmes suivants :

- AES (abréviation de l'expression anglaise « Advanced Encryption Standard »), travaillant sur des mots de 128 bits et offrant, à l'heure actuelle, une sécurité maximale,
- DES (abréviation de l'expression anglaise « Data Encryption Standard »), travaillant sur des mots de 64 bits, connu pour son universalité dans les systèmes les moins exigeants en matière de sécurité,
- 3DES (abréviation de l'expression anglaise « Triple Data Encryption Standard »), ou
- XDES (abréviation de l'expression anglaise « Extended Data Encryption Standard »), ces deux derniers algorithmes étant réputés pour des systèmes plus exigeant en terme de sécurité tout en assurant de hauts débits de chiffrement à faible coût.

Naturellement, le module de sécurisation CR permet de crypter des données plus longues que la longueur standard. Ce module est prévu pour traiter des données de 64 ou 128 bits enregistrées en huit ou seize mots de 8 bits, quatre ou huit mots de 16 bits, ou bien deux ou quatre mots de 32 bits respectivement dans la mémoire externe MEM, si bien qu'un accès à une de ces données est divisé en plusieurs accès de 8, 16 ou 32 bits respectivement.

A cet effet, le module de sécurisation CR peut exploiter les accès groupés ou accès consécutifs du contrôle de la mémoire cache du microprocesseur. Cette mémoire cache contient une copie partielle de la mémoire externe MEM qui est mise à jour en fonction de la partie du programme que le microprocesseur MIC exécute. La mémoire cache étant très rapide et très proche du microprocesseur MIC, elle permet généralement d'améliorer les performances du circuit.

Le remplacement des données présentes dans la mémoire cache au moyen du contrôleur de cache s'effectue par paquets, ces paquets ayant une taille minimale de 4 mots de 32 bits, ceci quelle que soit la taille des données traitées par le microprocesseur MIC.

On remarquera ici que la mémoire cache peut également être utilisée à d'autres fins par le circuit.

Il peut être imposé au contrôleur d'écrire les données enregistrées dans

la mémoire cache qui concernent la mémoire externe MEM, par paquets d'une taille multiple de 64 bits.

L'interfaçage de la mémoire cache avec la mémoire externe MEM qui n'est capable de gérer que des accès de 8, 16 ou 32 bits se fait de façon simple en scindant un accès de taille 64bits en huit accès de 8 bits, quatre accès de 16 bits ou deux accès de 32 bits respectivement.

Dans le cas d'accès 32 bits,L'algorithme DES ou 3DES sera ainsi chargé tous les 2 mots de 32 bits, tandis que l'algorithme AES sera chargé tous les 4 mots de 32 bits. Les données sont chargées à la volée. Dans le cas d'un traitement « pipeline » de l'algorithme AES, autrement dit lorsque le traitement complet d'une donnée en un ou plusieurs cycles est capable de recevoir une nouvelle donnée à chaque cycle, seul le premier accès introduit un temps de latence sur le temps total du transfert des données.

La clé privée utilisée par l'algorithme est stockée de préférence dans un registre programmable une seule fois dit « OTP » (pour l'expression anglaise One Time Programmable). Si le circuit intégré IC est pourvu d'une mémoire non volatile de type flash, ce registre peut y être localisé.

L'exemple de réalisation de l'invention présenté ci-dessus a été choisi pour son caractère concret. Il ne serait cependant pas possible de répertorier de manière exhaustive tous les modes de réalisation que recouvre cette invention. En particulier, tout moyen décrit peut-être remplacé par un moyen équivalent sans sortir du cadre de la présente invention.

REVENDICATIONS

1) Circuit IC comprenant un microprocesseur MIC, un ensemble de périphériques comportant au moins une interface de communication UMI prévue pour un accès externe, lesdits périphériques PER hormis ladite interface de communication UMI étant reliés audit microprocesseur MIC par un bus d'interconnexion BUS,
caractérisé en ce qu'il comprend de plus un module de sécurisation CR relié d'une part audit bus d'interconnexion BUS et d'autre part à ladite interface de communication UMI par l'intermédiaire d'une liaison dédiée DL.

2) Circuit selon la revendication 1, caractérisé en ce que ladite interface de communication UMI est adaptée à une mémoire externe MEM.

3) Circuit selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que ledit module de sécurisation comporte des moyens de cryptage CR.

4) Circuit selon la revendication 3, caractérisé en ce que lesdits moyens de cryptage CR font appel à une clé privée.

5) Circuit selon l'une quelconque des revendications 3 ou 4 caractérisé en ce que, la longueur de la clé de cryptage étant supérieure à la longueur standard des données que traite ledit microprocesseur MIC, il comprend des moyens pour décomposer lesdits mots cryptés en données de longueur standard.

6) Circuit selon la revendication 4 caractérisé en ce que, comportant de plus une mémoire cache associé à un contrôleur, la longueur de la clé de cryptage étant supérieure à la longueur standard des données que traite ledit microprocesseur MIC, ledit module de sécurisation CR est prévu pour exploiter les accès consécutifs dudit contrôleur afin de décomposer lesdits mots cryptés en données de longueur standard.

7) Circuit selon l'une quelconque des revendications 3 à 6, caractérisé en ce que la clé de cryptage est stockée dans un registre programmable une seule fois.

8) Circuit selon la revendication 7 caractérisé en ce que, comprenant de plus une mémoire non volatile, ledit registre figure dans cette mémoire non volatile.

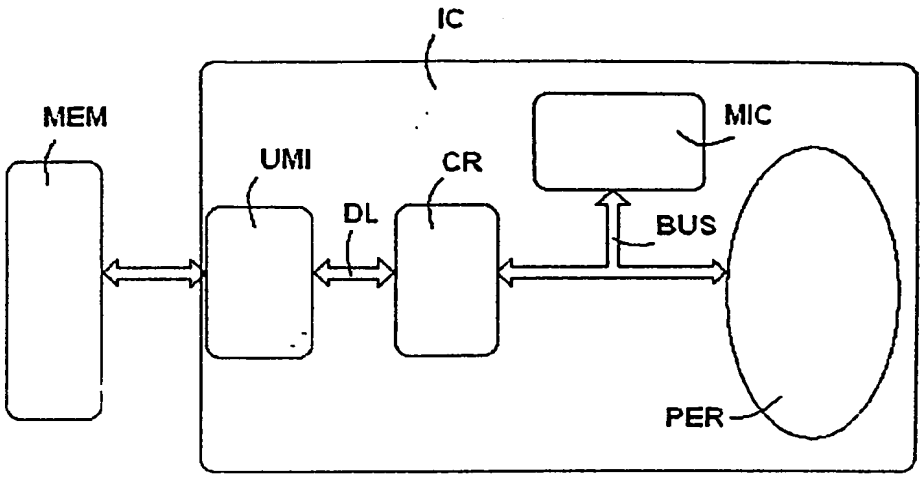

Figure unique

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/000718

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 172 731 A (FUJITSU LTD) 16 January 2002 (2002-01-16) page 2, line 1 - page 7, line 23 figure 1	1-8
X	EP 0 583 140 A (IBM) 16 February 1994 (1994-02-16) column 3, line 47 - column 9, line 6 figure 2	1-8

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 September 2004	28/09/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Segura, G

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/000718

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 908 810 A (GEN INSTRUMENT CORP) 14 April 1999 (1999-04-14) paragraph '0079! - paragraph '0091! paragraph '0102! - paragraph '0127! paragraph '0132! - paragraph '0151! paragraph '0162! paragraph '0193! - paragraph '0205! paragraph '0220! - paragraph '0227! figure 1	1-8
A	EP 0 556 928 A (TULIP COMPUTERS INTERNATIONAL) 25 August 1993 (1993-08-25) abstract column 1, line 13 - line 48	5,6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/000718

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1172731	A	16-01-2002	JP	2002032268 A	31-01-2002
			EP	1172731 A2	16-01-2002
			US	2002029345 A1	07-03-2002
EP 0583140	A	16-02-1994	US	5224166 A	29-06-1993
			DE	69327206 D1	13-01-2000
			DE	69327206 T2	08-06-2000
			EP	0583140 A1	16-02-1994
			JP	2085066 C	23-08-1996
			JP	6112937 A	22-04-1994
			JP	7107989 B	15-11-1995
EP 0908810	A	14-04-1999	US	6061449 A	09-05-2000
			CA	2249554 A1	10-04-1999
			CN	1236132 A	24-11-1999
			EP	0908810 A2	14-04-1999
			IL	126448 A	14-08-2002
			TW	445402 B	11-07-2001
EP 0556928	A	25-08-1993	NL	9200296 A	16-09-1993
			DE	69316046 D1	12-02-1998
			DE	69316046 T2	20-08-1998
			DK	556928 T3	07-09-1998
			EP	0556928 A1	25-08-1993
			ES	2113468 T3	01-05-1998
			US	5513262 A	30-04-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/000718

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 172 731 A (FUJITSU LTD) 16 janvier 2002 (2002-01-16) page 2, ligne 1 - page 7, ligne 23 figure 1 -----	1-8
X	EP 0 583 140 A (IBM) 16 février 1994 (1994-02-16) colonne 3, ligne 47 - colonne 9, ligne 6 figure 2 ----- -/--	1-8

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
17 septembre 2004	28/09/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Segura, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/000718

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 908 810 A (GEN INSTRUMENT CORP) 14 avril 1999 (1999-04-14) alinéa '0079! - alinéa '0091! alinéa '0102! - alinéa '0127! alinéa '0132! - alinéa '0151! alinéa '0162! alinéa '0193! - alinéa '0205! alinéa '0220! - alinéa '0227! figure 1 ----	1-8
A	EP 0 556 928 A (TULIP COMPUTERS INTERNATIONAL) 25 août 1993 (1993-08-25) abrégé colonne 1, ligne 13 - ligne 48 ----	5,6

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/000718

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1172731	A	16-01-2002	JP	2002032268 A	31-01-2002
			EP	1172731 A2	16-01-2002
			US	2002029345 A1	07-03-2002
EP 0583140	A	16-02-1994	US	5224166 A	29-06-1993
			DE	69327206 D1	13-01-2000
			DE	69327206 T2	08-06-2000
			EP	0583140 A1	16-02-1994
			JP	2085066 C	23-08-1996
			JP	6112937 A	22-04-1994
			JP	7107989 B	15-11-1995
EP 0908810	A	14-04-1999	US	6061449 A	09-05-2000
			CA	2249554 A1	10-04-1999
			CN	1236132 A	24-11-1999
			EP	0908810 A2	14-04-1999
			IL	126448 A	14-08-2002
			TW	445402 B	11-07-2001
EP 0556928	A	25-08-1993	NL	9200296 A	16-09-1993
			DE	69316046 D1	12-02-1998
			DE	69316046 T2	20-08-1998
			DK	556928 T3	07-09-1998
			EP	0556928 A1	25-08-1993
			ES	2113468 T3	01-05-1998
			US	5513262 A	30-04-1996